Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022

dell'8 dicembre 2017

Il Consiglio federale svizzero
ordina:

Riassunto

Per «infrastrutture critiche» (IC) s'intendono processi, sistemi e installazioni essenziali per il funzionamento dell'economia e per il benessere della popolazione. Vi rientrano ad esempio l'approvvigionamento energetico, i trasporti di persone e merci e le cure mediche. A livello di rischi correnti la Svizzera dispone in molti settori di un elevato livello di sicurezza: finora le perturbazioni gravi nell'erogazione di beni e servizi sono state sporadiche e di breve durata. Eventi come le brevi interruzioni di corrente che hanno colpito la città di Zurigo, il ponte danneggiato da un autocarro sull'autostrada A1 o il blackout che nel 2005 ha paralizzato la rete delle FFS, dimostrano tuttavia quanto siano vulnerabili la società e l'economia odierne. Un blackout generalizzato o una perturbazione di portata nazionale delle telecomunicazioni (p. es. di Internet) può paralizzare tutta l'economia, mettere fuori uso anche altre infrastrutture critiche (p. es. l'approvvigionamento alimentare o i servizi finanziari) e comportare gravi disagi per la popolazione (per il mancato funzionamento dell'approvvigionamento idrico, degli impianti di smaltimento delle acque luride, dell'illuminazione, dei riscaldamenti ecc.). I rischi per le infrastrutture sono aumentati in seguito all'incremento di catastrofi naturali, ad attacchi informatici sempre più raffinati, alle misure di risparmio di imprese e amministrazioni pubbliche e all'obsolescenza delle costruzioni.

Nel giugno del 2012, il Consiglio federale ha approvato una strategia nazionale per la protezione delle infrastrutture critiche (Strategia PIC) volta a migliorare ulteriormente la resilienza (capacità di resistenza, adattamento e rigenerazione) della Svizzera in materia di IC. Gli obiettivi generali e l'orientamento della presente strategia aggiornata sono gli stessi del 2012. L'aggiornamento della strategia PIC ha lo scopo di integrare i lavori principali, quali la tenuta di un inventario PIC periodicamente aggiornato, in un processo continuo, ancorarli nella legge e completarli puntualmente.

La Strategia nazionale PIC 2018–2022 definisce 17 misure volte a rafforzare la resilienza sia a livello settoriale, sia intersettoriale. La resilienza delle IC deve essere verificata in ogni settore e se necessario rafforzata. Ciò deve avvenire, da un lato, a livello dei gestori IC, che di regola dispongono di una gestione dei rischi e della continuità per assicurare l'operatività in caso d'evento. Tuttavia, per motivi economici questo è possibile solo fino a certo punto. I gestori IC devono quindi verificare la resilienza autonomamente, ad esempio in base alla Guida PIC esistente, e migliorarla se necessario. Dall'altro, le autorità specializzate, di vigilanza e di regolazione (conformemente all'allegato 1) nei diversi settori IC sono sollecitate a verificare congiuntamente se i provvedimenti adottati sono sufficienti o se sono necessarie ulteriori misure per migliorare la resilienza. A tal fine sono tenute a identificare e valutare, per ogni settore, le vulnerabilità e i rischi esistenti. Se necessario, occorre inoltre elaborare e attuare misure preventive e preparatorie supplementari volte a evitare eventuali interruzioni e a ripristinare rapidamente la normalità. La questione del grado di sicurezza e di resilienza delle infrastrutture critiche, nonché la definizione del quadro finanziario e giuridico per attuare eventuali misure di protezione supplementari necessarie dev'essere risolta, come finora, a livello

dei diversi settori politici (politica energetica, politica dei trasporti, sanità pubblica ecc.).

Per rafforzare la resilienza intersettoriale occorre ridurre la vulnerabilità della società, dell'economia e dello Stato rispetto a gravi perturbazioni e migliorare l'aiuto sussidiario ai gestori nella gestione di catastrofi e situazioni d'emergenza. A tal fine viene tenuto anche un inventario aggiornato delle infrastrutture critiche. Per sostenere i gestori di infrastrutture critiche particolarmente importanti nella gestione di situazioni d'emergenza, di crisi e della continuità, vengono ad esempio allestiti e periodicamente aggiornati i piani d'intervento preventivi dei partner della protezione della popolazione (polizia, pompieri, protezione civile ecc.) e dell'esercito.

La protezione delle infrastrutture critiche è un compito trasversale con interfacce verso diversi settori politici e operativi (politica energetica, politica di sicurezza, protezione contro i pericoli naturali, ecc.). Pertanto, la strategia nazionale PIC si applica principalmente nel quadro di strutture e competenze decentralizzate. Rimangono impregiudicate le competenze degli organi federali coinvolti, dei Cantoni, dei Comuni e dei gestori di IC. Nell'ambito dell'attuazione della strategia PIC sarà tuttavia presa in esame l'elaborazione di una base legale con direttive intersettoriali per i gestori di IC.

La presente strategia sarà verificata nel 2022 e aggiornata se necessario.

Indice

Riassunto **456**

1 Introduzione **460**
1.1 Contesto 460
1.2 Scopo, obiettivo e contenuto della strategia PIC 460
1.3 Destinatari della strategia PIC 461

2 Contesto **461**
2.1 Strategia nazionale PIC 2012 461
2.2 Interfacce con altri lavori 461
2.2.1 Strategia nazionale per la protezione della Svizzera contro i cyberrischi (SNPC) 462
2.2.2 Approvvigionamento economico del Paese (AEP) 462
2.2.3 Politica di gestione dei rischi della Confederazione 462

3 Campo d'applicazione **463**
3.1 Infrastrutture critiche 463
3.2 Protezione delle infrastrutture critiche 464

4 Vulnerabilità, rischi e misure di protezione **464**
4.1 Vulnerabilità 465
4.2 Rischi 465
4.3 Misure di protezione 465

5 Principi per la protezione delle infrastrutture critiche **466**

6 Principio e obiettivi della strategia nazionale PIC **467**
6.1 Principio 467
6.2 Obiettivi strategici 467
6.3 Applicazione operativa 468

7 Misure nell'ambito della strategia nazionale PIC **469**
7.1 Rafforzamento della resilienza infrasettoriale 469
7.2 Rafforzamento della resilienza a livello intersettoriale 472
7.2.1 Analisi 472
7.2.2 Valutazione 475
7.2.3 Misure (di protezione) 476
7.2.4 Attuazione e verifica 481

8 Attuazione della strategia nazionale PIC **482**
8.1 Strutture e competenze 482
8.2 Tempistica e controlling 483
8.3 Revisione della strategia PIC 484

Allegati:

1	Descrizione dei sottosettori e competenze per il rafforzamento della resilienza nei settori critici (Misura 1)	485
2	Panoramica delle misure, delle competenze e delle interfacce	488
3	Elenco delle abbreviazioni	490

Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022

1 Introduzione

1.1 Contesto

La Svizzera dipende dalla disponibilità continua di beni e servizi vitali quali l'energia, i trasporti e le telecomunicazioni. Gravi perturbazioni dell'approvvigionamento energetico, dei sistemi di trasporto, della sanità pubblica o della sicurezza pubblica causano ingenti danni sociali ed economici. La protezione delle infrastrutture critiche (PIC) riveste quindi grande importanza. Essa comprende tutte le misure necessarie per rafforzare la resilienza delle infrastrutture critiche (IC). Prevede ad esempio misure di tecnica edilizia, organizzative o amministrative nelle fasi di prevenzione, predisposizione operativa e gestione degli eventi. La protezione delle infrastrutture critiche non è un ambito politico a sé stante, ma piuttosto un compito trasversale con interfacce verso molti altri settori (politica energetica, politica dei trasporti, politica di sicurezza, pianificazione del territorio ecc.). La strategia PIC mira a migliorare il coordinamento dei compiti tra i diversi settori politici.

Nel giugno 2012, il Consiglio federale ha approvato la prima strategia nazionale PIC[1] e incaricato l'Ufficio federale della protezione della popolazione (UFPP) di coordinare l'attuazione delle misure ivi definite. Ha inoltre incaricato l'UFPP di verificare periodicamente la strategia PIC e di aggiornarla se necessario. Con la strategia nazionale PIC del 2012 sono state introdotte importanti misure per migliorare la resilienza. La presente strategia PIC riveduta è intesa a integrare tali lavori in un processo consolidato, ad ancorarli in un quadro giuridico e a completarli puntualmente. L'orientamento strategico nel settore PIC rimane però sostanzialmente invariato.

1.2 Scopo, obiettivo e contenuto della strategia PIC

La strategia nazionale PIC 2018–2020 è intesa a migliorare la resilienza (capacità di resistenza, adattamento e rigenerazione) della Svizzera in merito alle infrastrutture critiche. Essa contribuisce pertanto in modo determinante alla protezione della popolazione, alla salvaguardia del benessere economico e alla sicurezza del Paese.

La strategia definisce gli obiettivi perseguiti dalla Svizzera nel settore della PIC e illustra le misure necessarie per rafforzare la resilienza delle infrastrutture critiche della Svizzera. Delinea il campo d'applicazione, definisce quali sono le infrastrutture critiche per la Svizzera e fissa principi generali per la PIC. Stabilisce gli obiettivi prioritari e propone 17 misure da adottare nel settore PIC, in molti punti riprese dalla strategia 2012. Spiega infine in quali strutture e con quali competenze viene attuata la strategia. La presente strategia PIC sostituisce quella del 2012.

1 FF **2012** 6875

1.3 Destinatari della strategia PIC

La strategia nazionale PIC, varata dal Consiglio federale, definisce misure la cui attuazione compete in primo luogo alle unità organizzative dell'Amministrazione federale. Diverse misure concernono anche i Cantoni. Questi svolgono lavori PIC nell'ambito delle loro competenze e attribuzioni, nonché in conformità con le loro possibilità ed esigenze. La strategia concerne anche i gestori IC, la cui collaborazione è indispensabile per il raggiungimento degli obiettivi. La maggior parte dei gestori IC compiono già grossi sforzi per evitare interruzioni e perturbazioni. Il loro impegno nel verificare i provvedimenti adottati e nel migliorarli se necessario, nonché la loro disponibilità a collaborare con gli organi statali e gli altri gestori IC, sono di fondamentale importanza.

2 Contesto

2.1 Strategia nazionale PIC 2012

La strategia nazionale PIC del 2012 prevedeva complessivamente 15 misure. Il Consiglio federale è stato informato in merito allo stato d'attuazione di tali misure a fine 2016 in una nota informativa e un rapporto corrispondente. L'esperienza mostra che la strategia ha dato i suoi frutti e che va nella giusta direzione. Permane invece una necessità d'intervento sul piano della designazione dei settori e sottosettori critici e su quello delle misure. I lavori ancora necessari saranno illustrati in un rapporto dettagliato concernente la strategia nazionale PIC 2018–2022. Nella sezione dedicata alle misure del presente documento saranno indicati anche gli obiettivi raggiunti e le necessità d'intervento che ne derivano.

2.2 Interfacce con altri lavori

La protezione delle infrastrutture critiche è un compito trasversale con interfacce verso molti altri settori. Numerosi progetti e lavori in corso e previsti contribuiscono al raggiungimento degli obiettivi fissati nella strategia PIC. Di regola questi coprono solo una parte del ventaglio PIC, ad esempio singoli settori o singoli rischi (p. es. rischi cibernetici o pericoli naturali). I lavori nell'ambito della strategia PIC si fondano sulle basi esistenti e le completano se necessario in collaborazione con altri organi competenti. A titolo d'esempio citiamo la collaborazione con la strategia nazionale per la protezione della Svizzera contro i cyberrischi (SNPC), con l'approvvigionamento economico del Paese (AEP) e con la politica della Confederazione in materia di gestione dei rischi. Al momento dell'attuazione delle singole misure viene effettuato un censimento delle basi rilevanti e un'analisi congiunta delle misure ancora necessarie.

2.2.1 Strategia nazionale per la protezione della Svizzera contro i cyberrischi (SNPC)

Contemporaneamente alla strategia nazionale PIC, nel giugno 2012 il Consiglio federale ha varato anche la prima SNPC. Quest'ultima illustra come la Svizzera si protegge dagli attacchi cibernetici e in che modo rafforza la propria resilienza in questo campo. Dal 2012 al 2017 sono state attuate sedici misure nei settori prevenzione, reazione e continuità. A partire dal 2018 dovrebbe diventare effettiva la nuova NCS, elaborata in collaborazione con tutti i dipartimenti, l'economia privata e i Cantoni. Essa è intesa e continuare i lavori in corso e a svilupparli ulteriormente.

La protezione delle infrastrutture critiche dai cyber-rischi è parte integrante della NCS. Quest'ultima tratta gli aspetti dei cyber-attacchi della strategia PIC e attua le relative misure in stretto coordinamento con la strategia PIC.

2.2.2 Approvvigionamento economico del Paese (AEP)

Lo scopo dell'AEP è di garantire l'approvvigionamento della Svizzera con beni e servizi importanti. In caso di gravi impasse nell'approvvigionamento entrano in vigore le misure preventive (p. es. il ricorso alle scorte obbligatorie o la gestione di beni importanti come la corrente elettrica). L'AEP copre circa la metà dei settori e sottosettori critici della strategia nazionale PIC e contribuisce così in maniera determinante al raggiungimento dei suoi obiettivi. Le altre attività in campo PIC si limitano a sottosettori non coperti dall'AEP (p. es. autorità o organizzazioni di primo intervento) e ad aspetti non trattati dall'AEP. L'AEP si concentra essenzialmente su impasse di lunga durata a livello nazionale. Nel contesto della strategia PIC sono ormai considerate rilevanti anche perturbazioni di corta durata e quelle che non toccano tutta la Svizzera (p. es. interruzioni e perturbazioni a livello regionale).

2.2.3 Politica di gestione dei rischi della Confederazione

La gestione dei rischi è stata implementata nella Confederazione nel 2005. Essa è focalizzata su eventi che hanno gravi conseguenze negative sul raggiungimento degli obiettivi e sull'adempimento dei compiti dell'Amministrazione federale. È quindi particolarmente importante per il settore «Autorità». Sussistono però anche interfacce verso compiti delle autorità specializzate, di vigilanza e di regolazione della Confederazione in altri settori. La differenza essenziale rispetto alla PIC risiede nel fatto che non si tratta dei rischi per la popolazione e l'economia, ma di rischi per la Confederazione. Determinati rischi possono infatti essere rilevanti per la Confederazione ma non per la società e l'economia. Inoltre, in molti casi le infrastrutture critiche non sono di competenza esclusiva della Confederazione, ma anche o solo dei Cantoni e dei Comuni (approvvigionamento idrico, sanità pubblica ecc.). Al momento dell'attuazione delle diverse misure della strategia nazionale PIC viene accertato quali aspetti sono già coperti nell'ambito della gestione dei rischi della Confederazione e a quale livello è invece necessario intervenire.

3 Campo d'applicazione

Il campo d'applicazione della strategia nazionale PIC è dato dalla definizione dei concetti «infrastrutture critiche» e «protezione delle infrastrutture critiche» e dalla designazione delle infrastrutture critiche.

3.1 Infrastrutture critiche

Definizione del concetto di infrastrutture critiche: *per «infrastrutture critiche» (IC) s'intendono processi, sistemi e installazioni essenziali per il funzionamento dell'economia e per il benessere della protezione.*

La gamma delle infrastrutture critiche in Svizzera comprende i settori seguenti:

Tabella 1

Settori e sottosettori critici della Svizzera

Settori	Sottosettori
Autorità	Ricerca e insegnamento
	Beni culturali
	Parlamento, governo, giustizia, Amministrazione
Energia	Approvvigionamento di gas naturale
	Approvvigionamento di petrolio
	Approvvigionamento d'energia elettrica
	Teleriscaldamento e calore di processo
Smaltimento	Rifiuti
	Acque di scarico
Finanze	Servizi finanziari
	Servizi assicurativi
Sanità pubblica	Prestazioni mediche
	Servizi di laboratorio
	Chimica e agenti terapeutici
Informazione e comunicazione	Servizi informatici
	Telecomunicazioni
	Media
	Servizi postali
Alimentazione	Approvvigionamento alimentare
	Approvvigionamento idrico

Settori	Sottosettori
Sicurezza pubblica	Esercito
	Organizzazioni di primo intervento (polizia, pompieri, sanità)
	Protezione civile
Trasporti	Traffico aereo
	Traffico ferroviario
	Traffico navale
	Traffico stradale

Nell'allegato 1 viene precisato quali prestazioni e funzioni dei sottosettori sono particolarmente rilevanti dal punto di vista della PIC.

Nelle infrastrutture critiche rientrano fondamentalmente tutti gli elementi (gestori, sistemi informatici, impianti, costruzioni ecc.) che forniscono prestazioni in uno dei 27 sottosettori elencati nella tabella 1, indipendentemente dalla loro criticità (importanza). La criticità è una misura relativa che indica l'importanza dell'interruzione di un'infrastruttura critica per la popolazione e le sue basi vitali. Essa dipende dal livello considerato: un'IC può avere una criticità elevata a livello locale o comunale (p. es. una stazione di trasformazione nella rete di distribuzione della corrente elettrica), un'altra ha una criticità elevata anche a livello nazionale o internazionale (p. es. sistemi di gestione centralizzati della rete di trasporto).

3.2 Protezione delle infrastrutture critiche

La protezione delle infrastrutture critiche comprende le misure volte a ridurre la probabilità d'insorgenza e/o l'entità dei danni provocati da una perturbazione, un'interruzione o una distruzione di infrastrutture critiche e quindi la durata della loro mancata disponibilità. Queste misure devono sempre essere proporzionate all'importanza delle singole infrastrutture critiche. La PIC è quindi importate a tutti e tre i livelli statali: a livello federale, dove si dà la priorità all'infrastruttura critica d'importanza nazionale o addirittura internazionale, ma anche a livello cantonale o comunale, dove si dà la priorità alle infrastrutture critiche d'importanza cantonale o comunale.

4 Vulnerabilità, rischi e misure di protezione

I punti vulnerabili possono condurre all'interruzione delle infrastrutture critiche. Da queste vulnerabilità risultano dei rischi che possono essere ridotti con misure adeguate.

4.1 Vulnerabilità

Per essere funzionanti, le infrastrutture critiche dipendono dalla disponibilità di risorse come manodopera, materie prime, fonti d'energia e tecnologie dell'informazione e della comunicazione (TIC). Se un'avaria o la perdita di una risorsa chiave compromette il loro funzionamento, siamo in presenza di vulnerabilità rilevanti. Si distinguono i seguenti gruppi di risorse:

- manodopera: vi rientrano persone che sono di fondamentale importanza per il funzionamento delle infrastrutture critiche. Si tratta di persone chiave, specialisti ed esperti dei singoli processi;
- materiali di lavorazione e mezzi d'esercizio: vi rientrano materie prime, fonti d'energia (carburanti e combustibili), semi-fabbricati e prodotti finiti;
- servizi: vi rientrano la logistica (trasporti, infrastrutture edilizie) e i servizi nel campo dell'informatica (incl. dati) e dell'approvvigionamento energetico (p. es. corrente elettrica). Si deve tenere conto del fatto che i servizi rilevanti possono essere forniti sia in patria che all'estero. Molti servizi IC dipendono ad esempio da sistemi satellitari (p. es. GPS o Galileo). La vulnerabilità può nascere anche dalla presenza di pochi offerenti (monopolisti).

4.2 Rischi

Per le principali vulnerabilità occorre analizzare i rischi che ne derivano. Delle interruzioni significative possono essere causate sia da pericoli naturali che da pericoli antropici:

- pericoli naturali: gravi perturbazioni possono essere causate ad esempio da inondazioni, tempeste, valanghe o terremoti;
- pericoli tecnologici: vi rientrano i guasti ai sistemi, i blackout, una topologia di rete lacunosa;
- pericoli sociali: per la PIC sono ad esempio rilevanti gli atti di sabotaggio, il terrorismo o le pandemie. In seguito al crescente impiego di sistemi d'automazione e di comando, aumenta la minaccia di cyberattacchi.

Per stimare i rischi sono rilevanti la probabilità o la plausibilità di un pericolo e i danni per la popolazione e le sue basi vitali che derivano dalla perturbazione o dalla distruzione delle infrastrutture critiche. Grazie alle misure di protezione già implementate risultano rischi minori.

4.3 Misure di protezione

Per le misure da valutare e adottare si distingue tra misure preventive, misure di predisposizione e misure d'intervento. Con queste misure è possibile evitare le interruzioni o perlomeno garantire il funzionamento (continuità) e ridurre l'entità dei danni (ad esempio predisponendo processi sostitutivi o alternativi). Molto importanti

sono anche le misure volte a migliorare i preparativi della popolazione e dell'economia in vista di un'eventuale interruzione delle infrastrutture critiche.

Le misure di protezione sono attribuibili alle seguenti categorie:

- misure tecniche di costruzione: rafforzamento di edifici, acquisizione di generatori di corrente d'emergenza, segregazione di sistemi informatici ecc.;
- misure organizzative ed amministrative: istituzione di uno stato maggiore di crisi, esecuzione di controlli alle entrate, definizione di postazioni di lavoro alternative;
- misure giuridiche e normative: modifica di basi legali (legge, ordinanza, istruzioni ecc.);
- misure nel settore del personale: definizione di regole per le sostituzioni o la formazione e sensibilizzazione dei collaboratori.

Per tutti i gruppi di misure riveste inoltre grande importanza la protezione delle informazioni.

5 Principi per la protezione delle infrastrutture critiche

Approccio globale fondato sui rischi: la protezione delle infrastrutture critiche persegue un approccio globale e fondato sui rischi. Prende in considerazione e mette in correlazione tutte le vulnerabilità e i pericoli che potrebbero perturbare seriamente le infrastrutture critiche. Anche per l'elaborazione e l'adozione delle misure di protezione occorre seguire un procedimento globale e fondato sui rischi.

Proporzionalità: il rapporto tra costi e benefici (riduzione dei rischi) delle misure per la protezione delle infrastrutture critiche dev'essere ottimale. L'obiettivo non è quello di eliminare completamente tutti i rischi. Ciò sarebbe tecnicamente impossibile e comporterebbe oneri sproporzionati. Le misure scelte devono inoltre essere costituzionali e legittimate dalla legge. Sono infine da evitare distorsioni del mercato.

Responsabilità condivisa: la protezione delle infrastrutture critiche è un compito trasversale con interfacce verso diversi ambiti politici e campi d'attività. Tutti i responsabili vengono esortati a tenere conto della protezione delle infrastrutture critiche nel loro settore. È inoltre molto importante la disponibilità dei gestori delle infrastrutture critiche a verificare e rafforzare di propria iniziativa la loro resilienza. Anche la popolazione e l'economia, che dipendono dal buon funzionamento delle infrastrutture critiche, sono esortati a migliorare la loro resilienza. Una migliore preparazione (p. es. costituzione di scorte alimentari da parte delle economie domestiche o acquisizione di un gruppo elettrogeno d'emergenza da parte delle imprese) contribuisce in modo determinate a ridurre l'entità dei danni in caso di perturbazioni.

Collaborazione tra enti pubblici e privati: la protezione della infrastrutture critiche richiede una stretta collaborazione tra tutti gli attori coinvolti (autorità a livello federale, cantonale e comunale e gestori IC). Dove possibile, le misure di protezione

devono essere elaborate congiuntamente. La collaborazione tra settore pubblico e privato è particolarmente importante nell'ambito della stesura di norme e direttive e dello scambio di informazioni.

Mantenimento delle competenze e responsabilità: le direttive e le norme per i gestori delle infrastrutture critiche risultano in particolare dalla legislazione settoriale (p. es. nei settori dell'energia, dei trasporti, delle finanze ecc.). Con il sostegno della Confederazione (p. es. Polizia giudiziaria federale, Corpo delle guardie di confine o Servizio federale di sicurezza), i Cantoni sono, nell'ambito delle loro possibilità, responsabili tra l'altro della lotta contro i pericoli nell'ambito della sicurezza interna e della protezione della popolazione. Se necessario e secondo le disponibilità, l'esercito può sostenere le autorità civili nell'ambito di interventi sussidiari.

6 Principio e obiettivi della strategia nazionale PIC

6.1 Principio

Il principio su cui si fonda la strategia nazionale PIC è il seguente:

La Svizzera garantisce la resilienza delle infrastrutture critiche in modo da evitare, nel limite del possibile, gravi interruzioni su vasta scala e limitare i danni in caso d'evento.

Per resilienza s'intende la capacità di un sistema, di un'organizzazione o di una società di resistere a perturbazioni interne o esterne (capacità di resistenza) e di mantenere (capacità di adattamento) o ripristinare il più presto possibile e completamente il funzionamento (capacità di rigenerazione).

6.2 Obiettivi strategici

L'obiettivo principale della strategia nazionale PIC è di migliorare la resilienza della Svizzera dal profilo delle infrastrutture critiche. A tal fine, l'obiettivo principale è stato articolato nei seguenti obiettivi parziali:

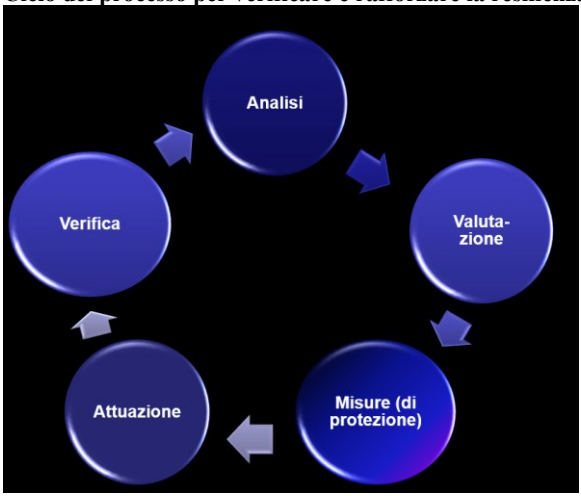
- le infrastrutture critiche sono resilienti in modo da evitare, nel limite del possibile, gravi interruzioni su vasta scala e ripristinare il più presto possibile il funzionamento in caso d'evento;
- la popolazione e l'economia sono resilienti in modo che le interruzioni e perturbazioni delle IC non possano causare danni importanti;
- le autorità sono preparate a reagire in modo appropriato a eventuali interruzioni delle IC;
- i gestori IC vengono sostenuti efficacemente nella gestione degli eventi.

6.3 Applicazione operativa

Il rafforzamento della resilienza si fonda su un processo a cinque livelli, composto dai seguenti elementi:

Figura 1

Ciclo del processo per verificare e rafforzare la resilienza



Analisi

- Identificare i processi, i sistemi, gli oggetti critici ecc.;
- identificare e analizzare le vulnerabilità e i rischi che potrebbero causare gravi interruzioni;
- individuare per tempo i cambiamenti rilevanti a livello di rischi e minacce per le infrastrutture critiche e comunicarli agli organi competenti.

Valutazione

- Individuare le divergenze dalle direttive vigenti e adottare le misure per colmare le lacune;
- definire il livello di sicurezza auspicato.

Misure (di protezione)

- Sono state definite e decise misure per:
  - evitare possibilmente gravi interruzioni;
  - far fronte agli eventi;
  - ripristinare rapidamente il funzionamento normale;
  - ridurre le conseguenze delle interruzioni.

Le misure presentano un rapporto ottimale tra costi e rischi residui.

Attuazione

– Le misure definite sono applicate nei tempi richiesti.

Verifica

– L'effetto delle misure adottate è verificato;
– le misure sono corroborate nell'ambito di esercitazioni e istruzioni.

Per rendere più resilienti le infrastrutture critiche della Svizzera, secondo il processo descritto occorre rafforzare sia la resilienza delle IC nei singoli settori (infrasettoriale), sia la resilienza trasversale ai settori (intersettoriale):

1. rafforzare la resilienza infrasettoriale: la resilienza dei singoli settori dev'essere verificata e, se del caso, migliorata. Secondo il procedimento descritto sopra, si tratta di analizzare le vulnerabilità e i rischi specifici alle diverse infrastrutture critiche al fine di adottare e attuare le misure atte a rafforzare la loro resilienza;
2. rafforzare la resilienza intersettoriale: si tratta di rafforzare la resilienza della popolazione, dell'economia e dello Stato per evitare interruzioni di infrastrutture critiche o di adottare le misure necessarie per aiutare i gestori a gestire gli eventi (a complemento delle misure infrasettoriali per il sostegno sussidiario dei gestori IC).

7 Misure nell'ambito della strategia nazionale PIC

In base agli obiettivi strategici e all'applicazione operativa (cfr. n. 6) vengono definite misure infra- e intersettoriali al fine di ricavarne un piano d'attuazione. Questo sarà completato con un piano d'attuazione dettagliato una volta approvata la strategia nazionale PIC. Nel quadro più ampio della protezione delle infrastrutture critiche sono già in corso o previsti numerosi progetti, piani e misure importanti. Nell'ambito dell'attuazione della strategia nazionale PIC si tratterà quindi spesso di verificare i processi già esistenti ed eventualmente di completarli. Nel limite del possibile, la strategia nazionale PIC si fonda su elementi già esistenti. Il confronto dettagliato con i progetti in corso è assicurato nell'ambito della pianificazione dell'attuazione. L'allegato 2 alla strategia offre un quadro generale dei provvedimenti e delle correlazioni con altri lavori in materia; nel testo si rinuncia volutamente ad una citazione esplicita.

7.1 Rafforzamento della resilienza infrasettoriale

Per rafforzare la resilienza del sistema globale delle infrastrutture critiche, è importante che il grado di resilienza di tutti i singoli componenti rilevanti (approvvigionamento di corrente elettrica, telecomunicazioni, trasporti stradali ecc.) sia proporzionale alla loro importanza. Sia dalla parte dei gestori IC, sia nei singoli settori, di regola sono già stati adottati numerosi provvedimenti volti a migliorare la resilienza (p. es. regolazioni infrasettoriali o misure predisposte ad esempio nell'ambito

dell'AEP). Per quanto concerne la resilienza infrasettoriale si tratta quindi di verificare se i provvedimenti adottati per raggiungere gli obiettivi secondo la strategia PIC siano sufficienti o se siano necessarie ulteriori misure. A tal fine vengono analizzate, conformemente al procedimento descritto al numero 6.3, le vulnerabilità e i rischi delle singole infrastrutture nonché elaborate e attuate, se necessario, misure di prevenzione e predisposizione operativa per ridurre i rischi.

Questi lavori vengono svolti in particolare a due livelli: da un lato, a livello dei singoli gestori IC. Questi dispongono in genere di unità di gestione dei rischi, come pure di unità di gestione delle emergenze, delle crisi e della continuità. Per garantire l'operatività anche in caso di catastrofi e situazioni d'emergenza vengono in parte adottati provvedimenti anche importanti. Non è tuttavia assicurato che i processi essenziali per la popolazione e l'economia siano prioritari anche per le imprese (focalizzate, queste ultime, soprattutto sul benessere economico). I gestori devono quindi, in collaborazione con le autorità specializzate, di vigilanza e regolazione, verificare di propria iniziativa nei singoli settori se i provvedimenti adottati siano sufficienti o se occorra rafforzare la resilienza. Per agevolare i gestori in questi lavori, l'UFPP ha pubblicato una guida e un sussidio per l'attuazione.

Le autorità specializzate, di vigilanza e di regolazione (conformemente all'allegato 1) nei diversi settori PIC sono sollecitate a verificare congiuntamente se i provvedimenti adottati siano sufficienti o se sussistano rischi sistemici di gravi interruzioni su vasta scala e se siano necessari provvedimenti per ridurli. Per questo, d'altro lato, si tratta di verificare la resilienza specifica di ciascun sottosettore critico (approvvigionamento di corrente elettrica, trasporto su rotaia, telecomunicazioni ecc.). Questo tenendo conto dei provvedimenti già adottati (da parte dei gestori o pianificazioni settoriali ad esempio dell'AEP) e verificando se sussistano rischi gravi che devono essere mitigati. In molti casi tali rischi possono essere ridotti con soluzioni interne ai singoli settori (p. es. accordi di collaborazione in caso d'evento). In determinate circostanze potrebbe anche essere necessario emanare direttive e norme supplementari per i gestori delle infrastrutture critiche. Spetta ai responsabili dei diversi settori politici (politica energetica, politica dei trasporti, politica sanitaria ecc.) definire le direttive corrispondenti e chiarire il finanziamento delle misure supplementari eventualmente necessarie. Nell'ambito della strategia nazionale PIC del 2012 e della SNPC sono state compiute analisi per tutti i sottosettori critici e adottate le prime misure. In circa la metà dei sottosettori i lavori coprono solo aspetti TIC (negli altri sottosettori critici si è tenuto conto di altre vulnerabilità e rischi rilevanti). Questi lavori devono quindi essere completati. È inoltre necessario aggiornare periodicamente queste e tutte le altre analisi poiché i rischi cambiano nel corso del tempo.

Dato che la strategia nazionale PIC non è giuridicamente vincolante né per i gestori IC né per le autorità specializzate, di vigilanza e regolazione nei vari settori, la verifica e il rafforzamento della resilienza delle infrastrutture critiche secondo le procedure descritte dipende unicamente dall'iniziativa individuale degli attori competenti. Vi sono inoltre singoli sottosettori (p. es. ospedali) per i quali, per mancanza di competenze federali, potrebbe risultare difficile creare o adeguare eventuali basi giuridiche. Una base legale con direttive intersettoriali in materia di resilienza delle IC potrebbe quindi semplificare notevolmente il raggiungimento degli obiettivi.

Questa dovrebbe coprire i sottosettori per i quali è stata individuata la necessità di una tale base legale e nei quali non vi sono altre possibilità per adottare le misure necessarie (p. es. con una soluzione settoriale o la creazione risp. l'adeguamento di una base legale settoriale).

Obiettivo:

– Le infrastrutture critiche in tutti i settori critici hanno un grado di resilienza proporzionale alla loro importanza. Tutti i rischi rilevanti sono identificati e le misure per raggiungere un livello ottimale di sicurezza definite e attuate. Lo spettro dei pericoli e delle misure preso in considerazione è il più ampio possibile.

Misura 1:

– Per le infrastrutture critiche per le quali non sono ancora stati effettuati i relativi lavori, devono essere svolte le analisi dei rischi e delle vulnerabilità conformemente al procedimento descritto al numero 6.3 ed elaborate e attuate misure per rafforzare la resilienza. Questi lavori devono essere periodicamente aggiornati.

Attuazione:

– I gestori IC verificano e rafforzano la loro resilienza, ad esempio sulla base della guida PIC, sia autonomamente che in collaborazione con le autorità specializzate, di vigilanza e di regolazione. L'UFPP sostiene metodicamente questi lavori nel limite del possibile.

– Le autorità specializzate, di vigilanza e di regolazione completano le analisi della vulnerabilità e le pianificazioni delle misure per i sottosettori critici che finora tenevano conto solo di aspetti TIC con ulteriori pericoli rilevanti (cfr. allegato 1). I lavori esistenti che coprono un ventaglio completo di vulnerabilità, rischi e misure, vengono aggiornati ogni quattro anni. Gli organi citati nell'allegato 1 decidono quale ente è responsabile. Se necessario l'UFPP può sostenere i lavori.

Misura 2:

– Occorre valutare la possibilità di creare una base legale per emanare le direttive intersettoriali per la resilienza delle infrastrutture critiche. Questa base legale deve coprire i settori per i quali è stata rilevata la necessità nell'ambito degli accertamenti a livello dei sottosettori critici.

Attuazione:

– Il DDPS (UFPP) valuta con gli attori competenti (in part. DEFR, DATEC e DFF) l'elaborazione di una proposta per una base legale intersettoriale con le direttive necessarie per rafforzare la resilienza delle infrastrutture critiche. Si tratta in particolare di valutare se le competenze si sovrappongono con le vigenti direttive e regolamentazioni infrasettoriali.

7.2 Rafforzamento della resilienza a livello intersettoriale

Le misure per rafforzare la resilienza intersettoriale contemplano tutte le attività necessarie per la concezione, il coordinamento e lo sviluppo delle attività rilevanti per la protezione delle infrastrutture critiche. S'intende in particolare rafforzare la resilienza della società, dell'economia e dello Stato e adottare misure volte a sostenere i gestori IC nel far fronte agli eventi. Gli obiettivi e le misure si basano sul processo esposto al numero 6.3.

7.2.1 Analisi

Analisi del campo d'intervento:
identificare e priorizzare le infrastrutture critiche

Prima di adottare delle misure di protezione, gli organi competenti devono sapere quali infrastrutture sono particolarmente critiche. Conoscere le infrastrutture critiche e la loro rilevanza è importante per valutare la situazione e per priorizzare le misure di protezione in caso di catastrofi e situazioni d'emergenza. Per la strategia nazionale PIC del 2012 è stato quindi allestito un inventario delle opere infrastrutturali critiche (inventario PIC). Questo comprende gli edifici e gli impianti che assumono grande importanza strategica a livello nazionale o cantonale. Nel suo insieme è classificato come SEGRETO. Singoli estratti che comprendono solo una parte delle informazioni (p. es. di un Cantone o un settore) di regola sono classificati come CONFIDENZIALI. I suoi dati devono essere periodicamente aggiornati. Oltre agli edifici e agli impianti rilevanti, nell'inventario PIC verranno aggiunti anche i gestori (imprese) di IC e i sistemi informatici critici. Nel limite del possibile si ricorre a dati già rilevati nell'ambito di altri elenchi.

Obiettivo:

– Le infrastrutture critiche della Svizzera sono identificate, censite, e aggiornate con i dati attuali, nel rispetto delle prescrizioni sulla protezione delle informazioni e dei dati. Sono individuati e priorizzati in particolare gli edifici e gli impianti come pure i sistemi e i gestori.

Misura 3:

– L'inventario PIC della Svizzera deve essere periodicamente aggiornato e completato con informazioni sui sistemi IT e i gestori critici.

Attuazione:

– L'UFPP è responsabile di individuare, in collaborazione con i servizi specializzati e i gestori, le infrastrutture critiche rilevanti dal punto di vista nazionale e di aggiornare periodicamente i dati. Per inserire la collaborazione in un quadro giuridico l'UFPP esamina la creazione di una relativa base legale nella LPPC. I Cantoni procedono nello stesso modo per le infrastrutture critiche rilevanti dal punto di vista cantonale.

Analisi del campo d'intervento:
conoscere i rischi, la vulnerabilità e le possibilità di protezione

Per rafforzare la resilienza delle infrastrutture critiche è necessario disporre di analisi intersettoriali dei rischi significativi. A tal fine, occorre raccogliere le analisi dei diversi sottosettori critici per riunirle in un quadro d'insieme dei rischi.

Per lo sviluppo metodologico sono inoltre necessari dati scientifici fondati, ad esempio nei settori delle interdipendenze e delle analisi di criticità. Bisogna inoltre seguire lo sviluppo delle nuove tecnologie e altri sviluppi (ambiente, contesto generale) che potrebbero generare nuovi rischi. Ciò avviene nell'ambito della ricerca settoriale degli organi federali e dei Cantoni.

Obiettivi:

- È disponibile un quadro d'insieme consolidato delle vulnerabilità e dei rischi associati alle infrastrutture critiche con indicazione della necessità d'intervento.
- Sono disponibili basi scientifiche fondate note agli attori rilevanti che consentono uno sviluppo sistematico della protezione delle infrastrutture critiche.

Misura 4:

- I risultati della verifica e del rafforzamento della resilienza dei sottosettori critici devono essere raccolti in un quadro d'insieme dei rischi.

Attuazione:

- Il DDPS (UFPP) consolida, in collaborazione con il DFF (ODIC e AFF) e il DEFR (UFAE), i risultati delle analisi dei singoli sottosettori.

Misura 5:

- Occorre approfondire la ricerca fondamentale su temi intersettoriali (p. es. interdipendenze e sviluppi in campo tecnologico, ambientale e contestuale).

Attuazione:

- Gli uffici federali, i Cantoni e i gestori sono responsabili della ricerca settoriale nella loro sfera di competenze. Il DDPS (UFPP) è responsabile della ricerca fondamentale intersettoriale in campo PIC.

Analisi del campo d'intervento:
migliorare la collaborazione e lo scambio di informazioni

Le infrastrutture critiche presentano un elevato grado d'interdipendenza. La collaborazione e il dialogo sui rischi e sulle possibili misure di protezione («best practices») tra i diversi rappresentanti dei settori delle infrastrutture critiche sono quindi di fondamentale importanza. Nell'ambito della strategia nazionale PIC del 2012 sono state create tre piattaforme (piattaforma dei gestori delle infrastrutture critiche nazionali, gruppo di lavoro PIC degli organi federali, interlocutori PIC cantonali). L'esperienza dimostra che la collaborazione intersettoriale e intercantonale nel

settore PIC riscuote molto interesse. Le piattaforme offrono a tutte le parti interessate dei diversi settori (organi federali e gestori IC) e ai Cantoni la possibilità di scambiare esperienze e discutere possibili soluzioni. Dato che le infrastrutture critiche costituiscono spesso dei sistemi transfrontalieri, occorre attribuire la necessaria importanza anche alla collaborazione internazionale. Lo scambio relativo ai cyber-rischi ha luogo tramite la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI).

Obiettivo:

– Occorre creare piattaforme intersettoriali che permettono di migliorare la collaborazione e promuovere lo scambio di informazioni sui rischi, sulle vulnerabilità e sulle possibili misure di protezione («best practices»).

Misura 6:

– Le piattaforme esistenti vengono mantenute e la collaborazione al loro interno intensificata se necessario. La composizione delle piattaforme viene verificata periodicamente.

Attuazione:

– Il DDPS (UFPP) coordina la piattaforma dei gestori di IC nazionali, gli interlocutori PIC cantonali e il gruppo di lavoro PIC delle autorità (Confederazione e Cantoni). A livello internazionale il DDPS (UFPP) rappresenta il punto di riferimento per le questioni PIC. La collaborazione internazionale in materia di cyber-rischi avviene tramite la Centrale MELANI.

Analisi del campo d'intervento:
individuare e comunicare precocemente pericoli e minacce acuti

In caso di pericoli e minacce gravi è importante che i gestori delle infrastrutture critiche siano informati per tempo in modo da adeguare il loro dispositivo di sicurezza. Da parte loro, i gestori devono informare rapidamente le organizzazioni di crisi della Confederazione, dei Cantoni e gli altri gestori IC in caso di una perturbazione. La legge sulle attività informative (LAIn) costituisce una base importante per l'identificazione delle minacce, comprese quelle per le infrastrutture critiche. Per altri tipi di minacce e pericoli (p. es. per i cyber-rischi o le catastrofi naturali) esistono già altre forme di collaborazione volte ad informare tempestivamente i gestori IC in caso d'evento (p. es. cerchie di clienti chiuse di MELANI). Occorre verificare periodicamente che i gestori di IC rilevanti di caso in caso siano coinvolti nei processi corrispondenti. Per le autorità è inoltre importante essere informati per tempo in merito a interruzioni e incidenti rilevanti dal punto di vista della sicurezza presso le infrastrutture critiche, affinché possano tracciare un quadro completo della situazione e disporre per tempo le misure per far fronte all'evento. Nell'ambito della protezione della popolazione, con NetAlert sussiste un sistema di comunicazione per segnalare le perturbazioni o interruzioni su base volontaria. In alcuni sottosettori i gestori IC sono inoltre tenuti a segnalare le perturbazioni all'autorità specializzata competente.

Obiettivo:

– I gestori IC rilevanti vengono informati per tempo e con uno standard qualitativo conforme alla loro importanza. Da parte loro, i gestori delle infrastrutture critiche comunicano perturbazioni e interruzioni significative alle autorità federali e cantonali competenti. La protezione delle informazioni e dei dati deve sempre essere garantita.

Misura 7:

– Verificare periodicamente i processi d'informazione in caso d'evento specifici per i singoli pericoli in merito al coinvolgimento dei gestori IC e adattarli se necessario.

Attuazione:

– Il DDPS (UFPP) verifica, in collaborazione con gli organi responsabili per i singoli pericoli (p. es. MELANI), se i gestori IC rilevanti sono coinvolti nei processi corrispondenti e se necessario elabora proposte di miglioramento.

Misura 8:

– Occorre elaborare una proposta di basi legali volte a obbligare i gestori a segnalare gravi incidenti o guasti funzionali alle autorità competenti.

Attuazione:

– Il DDPS (UFPP) valuta, in collaborazione tra gli altri con il DFF (ODIC) e il DATEC, la possibilità di elaborare delle basi legali per la segnalazione obbligatoria di gravi incidenti e interruzioni delle infrastrutture critiche. Questa deve coprire i settori che non possono essere disciplinati nelle basi legali specifiche. In particolare, occorre definire dei criteri per decidere a partire da quale livello di gravità è necessario segnalare l'evento.

7.2.2 Valutazione

Nell'ambito della valutazione si tratta in primo luogo di verificare se le eventuali direttive settoriali in materia di resilienza siano rispettate. In secondo luogo si deve garantire un livello di sicurezza armonizzato tra i vari settori. Gli obiettivi strategici generali sono enunciati al numero 6. L'obiettivo principale della protezione delle infrastrutture critiche è quello di raggiungere per ogni infrastruttura critica un grado di resilienza proporzionale alla sua importanza e alla sua ubicazione. Le direttive in materia di sicurezza per le singole infrastrutture critiche non devono quindi definire obiettivi di protezione fissi sotto forma di valori limite (p. es. durata massimo d'interruzione tollerata). Per ogni infrastruttura critica occorre invece fissare un livello di sicurezza basato sui rischi. In ogni singolo caso è fondamentale che venga raggiunto un rapporto ottimale tra i costi delle misure di protezione e i rischi residui risultanti dalle interruzioni delle infrastrutture critiche. Per fissare il livello di sicurezza ci si basa sulla disponibilità della società a investire nell'aumento della sicurezza (p. es. per evitare fatalità o danni economici in caso d'evento). Più alto è

l'importo investito, più mezzi sono disponibili per le misure di sicurezza, e più elevato sarà il livello di sicurezza. È quindi fondamentale che la disponibilità a investire per evitare danni in caso di interruzione di infrastrutture critiche sia la stessa in tutti i settori. Degli esempi corrispondenti sono riportati tra l'altro nella Guida PIC. Questi possono essere applicati nei sottosettori critici o dai gestori IC. Occorre tuttavia tenere conto che il livello concreto di sicurezza auspicato viene fissato solo al momento della pianificazione delle misure. L'obiettivo deve consistere nell'ottenere un rapporto ottimale tra costi delle misure e costi risultanti dai rischi residui. Se le relative misure saranno attuate permettendo di raggiungere il livello ottimale di sicurezza o meno dipende dalle decisioni della politica e della società. Occorre quindi sempre una valutazione accurata, che tenga conto anche di altri aspetti come la protezione della natura, la sostenibilità, la limitazione della libertà economica ecc.

Obiettivo:

– Raggiungere un livello di sicurezza armonizzato tra i vari settori che tenga conto in particolare della diversa importanza (criticità) delle singole IC.

Misura 9:

– Le basi esistenti relative al livello di sicurezza devono essere verificate se necessario.

Attuazione:

– Il DDPS (UFPP) verifica, se necessario in collaborazione con il DATEC (tra l'altro UFAM) e gli organi specializzati competenti, le proposte per il livello di sicurezza auspicato. Un'eventuale prescrizione legale intersettoriale in relazione alla resilienza delle infrastrutture critiche (misura M2) garantirebbe la volontà di aspirare a un livello di sicurezza armonizzato in tutti i settori critici.

7.2.3 Misure (di protezione)

Campo d'intervento Misure (di protezione):
creare le basi per evitare interruzioni di infrastrutture critiche

Su scala intersettoriale è possibile adottare diverse misure per ridurre i rischi rilevanti per molte infrastrutture critiche e per evitare gravi interruzioni. Tali rischi generici concernono ad esempio il personale responsabile dell'esecuzione dei processi chiave. Per soddisfare gli elevati standard di sicurezza e per consentire lo scambio di informazioni classificate, queste persone dovrebbero essere sottoposte a un controllo di sicurezza riferito alla loro funzione. Secondo la legislazione vigente, attualmente ciò è possibile solo in casi eccezionali o attraverso la modifica di basi giuridiche infrasettoriali. Il controllo di sicurezza relativo alle persone non è l'unica misura importante nel settore del personale per garantire la sicurezza. È ad esempio necessario istruire e sensibilizzare le persone in materia di sicurezza integrale.

Per evitare interruzioni di infrastrutture critiche, le risorse rilevanti per il loro funzionamento devono possibilmente essere disponibili senza interruzioni. Nell'ambito della strategia nazionale PIC del 2012 sono state quindi elaborate diverse raccomandazioni per prioritizzare le infrastrutture critiche in caso di penuria di beni e servizi essenziali (p. es. in caso di penuria di elettricità). Si tratta di adottarle e di aggiornarle periodicamente.

I lavori svolti finora per verificare e rafforzare la resilienza delle infrastrutture critiche hanno dimostrato che quasi tutte queste infrastrutture dipendono dall'approvvigionamento energetico e da reti di telecomunicazione affidabili e che i rischi maggiori derivano quindi da blackout d'ampia portata e interruzioni delle telecomunicazioni. Se dal punto di vista economico e tecnico non è possibile o ragionevole realizzare una rete alternativa per l'alimentazione di corrente, nel settore delle telecomunicazioni si prevede invece di creare una rete per la comunicazione di dati autonoma, altamente affidabile e sicura per gli organi di condotta federali e cantonali e i gestori di infrastrutture critiche. La realizzazione di questa rete è prioritaria soprattutto per la protezione delle infrastrutture critiche.

Obiettivi:

- Il personale che ha accesso ai processi chiave nel settore delle infrastrutture critiche deve poter essere sottoposto a un controllo di sicurezza conforme alla sua funzione;
- in caso d'interruzione o di penuria di beni e servizi essenziali, nel limite delle possibilità tecniche si tiene prioritariamente conto delle infrastrutture critiche;
- è disponibile una rete dati e di comunicazione a prova d'interruzione («fail safe») a cui collegare i gestori delle infrastrutture critiche, che in caso d'interruzione delle telecomunicazioni pubbliche devono essere in grado di garantire la preservazione dei processi rilevanti per il funzionamento delle loro infrastrutture e di comunicare con gli altri gestori e le organizzazioni federali e cantonali competenti per la gestione delle crisi.

Misura 10:

- Occorre elaborare una proposta di base legale per regolamentare il controllo di sicurezza del personale addetto alle infrastrutture critiche e di altre persone autorizzate ad accedervi.

Attuazione:

- Il DDPS (UFPP in collaborazione con la SIO) valuta la creazione di una base legale intesa a regolamentare il controllo di sicurezza su personale chiave dei gestori IC e altri titolari di autorizzazione d'accesso.

Misura 11:

- Rielaborare conformemente alle raccomandazioni le basi per la prioritizzazione in caso di interruzioni e situazioni di penuria di beni e servizi essenziali.

Attuazione:

– Gli organi competenti (tra cui il DEFR [UFAE]) attuano le raccomandazioni per priorizzare le infrastrutture critiche in caso di interruzioni e situazioni di penuria in collaborazione con il DDPS (UFPP).

Misura 12:

– Occorre realizzare una rete alternativa a prova d'interruzioni («fail safe») e creare le basi necessarie per collegare i gestori di infrastrutture critiche a questa rete. Per assicurare la comunicazione vocale, gestori IC scelti vengono allacciati alla rete radio nazionale di sicurezza POLYCOM.

Attuazione:

– Il DDPS (UFPP) realizza, sulla base della Rete di condotta svizzera dell'esercito e in collaborazione con altri organi federali e cantonali, la rete di dati sicura (RDS) e definisce le basi per l'allacciamento dei gestori IC. Si tratta in particolare di decidere quali gestori possono essere collegati alla rete e quali condizioni tecniche e finanziarie devono soddisfare. Se necessario, gestori IC scelti vengono allacciati alla rete radio nazionale di sicurezza POLYCOM nell'ambito del sistema di comunicazione d'emergenza dell'AEP.

Campo d'intervento Misure (di protezione):
migliorare la preparazione della popolazione, dell'economia e dello Stato a interruzioni e situazioni di penuria di beni essenziali

Gravi interruzioni delle infrastrutture critiche possono comportare gravi disagi per la popolazione e compromettere seriamente il funzionamento dell'economia e dello Stato. L'entità dei danni può essere ridotta se la popolazione, l'economia e lo Stato sono adeguatamente preparati. Per questo motivo si attribuisce grande importanza alle pianificazioni preventive per la gestione degli eventi e alla sensibilizzazione preliminare della popolazione e dell'economia sui possibili rischi e sulle misure preventive individuali. Considerata l'importanza cruciale dell'approvvigionamento d'elettricità, i piani per gestire blackout o penurie di corrente sono prioritari. A tal fine sono in corso numerosi lavori a livello federale e cantonale. Questi devono essere periodicamente aggiornati. Nell'ambito dell'approvvigionamento economico del Paese e di Alertswiss sono stati realizzati numerosi prodotti per sensibilizzare la popolazione e le imprese (p. es. Guida corrente elettrica per l'economia e la popolazione, modello di piano d'emergenza personale ecc.).

Obiettivo:

– La popolazione, l'economia e lo Stato sono preparati in vista di gravi interruzioni di infrastrutture critiche, in modo tale da permettere di ridurre gli effetti e di gestire l'evento.

Misura 13:

– La Confederazione e i Cantoni elaborano pianificazioni preventive per la gestione di gravi interruzioni di infrastrutture critiche (in particolare per il caso di blackout) e le aggiornano periodicamente.

Attuazione:

– Le autorità federali competenti della Confederazione elaborano pianificazioni preventive per la gestione di interruzioni di infrastrutture critiche. A livello cantonale queste pianificazioni vengono allestite nell'ambito delle analisi dei pericoli e della predisposizione operativa. Il DDPS (UFPP) stila un elenco delle pianificazioni preventive esistenti e lo aggiorna periodicamente.

Misura 14:

– La popolazione e l'economia vengono informate e sensibilizzate in merito alle possibilità di prevenzione personali in caso di interruzione di infrastrutture critiche, in particolare di blackout.

Attuazione:

– Il DEFR (UFAE) aggiorna e completa se necessario i prodotti d'informazione e di sensibilizzazione relativi a interruzioni dell'approvvigionamento di corrente elettrica e dei sistemi di telecomunicazione. Il DDPS (UFPP) realizza, nell'ambito di Alertswiss e in collaborazione con altri enti (tra l'altro UFAE e Cantoni), i prodotti per sensibilizzare la popolazione in materia di autoprevenzione.

Campo d'intervento Misure (di protezione): aiutare i gestori di infrastrutture critiche a gestire gli eventi

In caso di minacce o pericoli acuti o di gravi interruzioni, è importante che le autorità aiutino i gestori IC a gestire l'evento in modo possibilmente efficace con mezzi o conoscenze sussidiari extra-aziendali[2]. In questo modo è possibile evitare che un'interruzione (ad esempio durante un'inondazione) causi danni supplementari alla popolazione e all'economia o ad altre infrastrutture critiche (effetto domino).

Per i rischi convenzionali sono disponibili, in quantità limitata, mezzi della polizia, dei pompieri, della sanità, della protezione civile e dell'esercito. In caso di eventi in cui sono coinvolte sostanze chimiche, biologiche o radiologiche, l'UFPP dispone inoltre di mezzi sussidiari (squadra d'intervento DDPS) per sostenere le forze d'intervento in loco. Trattandosi di uno tra i numerosi altri compiti per le organizzazioni d'intervento, la PIC non può fungere da unica base per dedurre parametri precisi. Dal momento che l'elenco delle infrastrutture critiche minacciate dipende dall'evento, è impossibile definire in anticipo le priorità o un numero minimo di oggetti da proteggere imperativamente. Si tratta piuttosto di garantire che i mezzi disponibili vengano impiegati in modo efficiente in caso d'evento. In questo conte-

2 Ad esempio con forze d'intervento (polizia, pompieri, protezione civile, esercito), mezzi di comunicazione o gruppi elettrogeni d'emergenza.

sto può offrire un valido contributo la gestione delle risorse a livello federale (ResMaB) e cantonale (ResMaK). Sul piano strategico, le priorità nell'ambito dell'aiuto sussidiario devono essere fissate tenendo conto dell'importanza (criticità) delle infrastrutture critiche, delle minacce e dei mezzi disponibili. Nella maggior parte dei casi sarà possibile proteggere solo un numero esiguo di infrastrutture critiche, ossia le più importanti. È quindi indispensabile che i gestori abbiano adottato valide misure preventive e dispongano di un sistema di gestione delle crisi e della continuità efficaci (come nell'obiettivo posto dalla misura 1). Non meno importante è la collaborazione settoriale e intersettoriale tra i gestori IC.

Fissare le priorità è un compito difficile per le organizzazioni d'intervento statali, poiché la competenza dei mezzi operativi per la difesa contro i pericoli con mezzi di polizia e per la protezione della popolazione, spetta ai Cantoni e ai comuni. Molte infrastrutture critiche sono però sistemi interconnessi gestiti a livello nazionale o addirittura internazionale (p. es. rete di trasmissione della corrente elettrica). È quindi importante che venga effettuata una valutazione globale a livello nazionale a seconda dell'evento. Oltre alle organizzazioni di crisi settoriali (p. es. in ambito AEP), assume un ruolo centrale anche lo Stato maggiore federale Protezione della popolazione (SMF PP). La collaborazione con i gestori IC viene attualmente regolamentata e intensificata nel quadro di un'ordinanza. La cooperazione con gli organi di condotta competenti è importante anche a livello locale, regionale e cantonale, anche tenuto conto del fatto che la collaborazione a questi livelli è spesso già consolidata.

A differenza di quanto avviene per i rischi convenzionali, per aiutare i gestori a far fronte ai cyber-rischi per ora sono disponibili pochissimi mezzi sussidiari civili e militari. Visto che anche in questo caso la protezione delle infrastrutture critiche è solo un compito parziale, le competenze necessarie devono essere garantite nei diversi campi d'attività (politica di sicurezza, SNPC, sviluppo ulteriore dell'esercito ecc.). Di conseguenza, si tratta anche qui, nel quadro dei mezzi disponibili, di tenere conto dell'importanza delle infrastrutture critiche per fissare le priorità.

Per garantire una gestione degli eventi possibilmente efficace si deve quindi disporre di pianificazioni preventive d'intervento aggiornate. L'esercito e più Cantoni hanno già elaborato dei piani corrispondenti per oggetti dell'Inventario PIC particolarmente importanti. Nell'ambito dell'aiuto da parte dell'esercito, i piani coprono però soltanto la protezione di edifici e impianti contro aggressioni perpetrate da terzi. Servono però anche piani per mezzi supplementari (p. es. eventuali mezzi cibernetici).

Obiettivo:

– I gestori delle infrastrutture critiche vengono sostenuti, tenendo conto della loro importanza, in modo sussidiario ed efficace con mezzi esterni al fine di combattere le minacce, garantire un funzionamento minimo e un rapido ritorno alla normalità.

Misura 15:

– Analizzare, d'intesa con gli organi interessati, e se necessario ottimizzare i processi relativi all'attribuzione di mezzi esterni per sostenere i gestori nella

gestione degli eventi. I processi e le competenze vengono comunicati agli organi coinvolti (in particolare ai gestori IC).

Attuazione:

– Il DDPS (UFPP) verifica i processi esistenti in collaborazione con altri organi del DDPS (SG, Aggruppamento Difesa), con il DFGP e con il DFF e eventualmente elabora, d'intesa con gli enti specializzati rilevanti, proposte per ottimizzare questi processi.

Misura 16:

– Occorre elaborare e aggiornare periodicamente piani d'intervento preventivi per la protezione delle infrastrutture critiche.

Attuazione:

– I Cantoni elaborano, ad esempio nell'ambito dell'analisi e della prevenzione cantonale dei pericoli, piani civili nel settore della protezione della popolazione per infrastrutture critiche scelte. Il DFF (ODIC) esamina, in collaborazione con il DDPS (SG), l'elaborazione di piani d'intervento civili e militari in relazione ai cyber-rischi. I piani civili e militari sono aggiornati periodicamente.

7.2.4 Attuazione e verifica

L'attuazione delle misure definite nella presente strategia dev'essere controllata e pilotata. Occorre inoltre verificare l'efficacia delle diverse misure. I compiti corrispondenti verranno esposti in un documento separato dopo l'approvazione della presente strategia. È infine importante testare la protezione delle infrastrutture critiche nell'ambito di esercitazioni.

Obiettivo:

– L'efficacia delle misure per la protezione delle infrastrutture critiche viene testata nell'ambito di esercitazioni.

Misura 17:

– Nell'ambito delle esercitazioni già pianificate (esercitazioni della rete integrata per la sicurezza, esercitazioni di condotta strategica della Confederazione, esercitazioni cantonali, simulazioni, ecc.) si devono addestrare anche singoli aspetti PIC.

Attuazione:

– Gli organi responsabili presso la Confederazione, i Cantoni e i gestori IC tengono conto degli aspetti PIC nella pianificazione e nello svolgimento delle esercitazioni. Gli insegnamenti tratti dalle esercitazioni riconfluiscono nei lavori in ambito PIC. Il DDPS (UFPP) sostiene questi organi consigliandoli se necessario.

8 Attuazione della strategia nazionale PIC

8.1 Strutture e competenze

L'attuazione della strategia nazionale PIC 2018–2022 si inserisce sostanzialmente nel quadro delle strutture e delle competenze esistenti. Nei relativi lavori, coordinati dal Segretariato PIC dell'UFPP, sono coinvolte sin dall'inizio le autorità federali e cantonali rilevanti, il settore economico (in particolare i gestori di infrastrutture critiche) e il mondo scientifico.

Il Segretariato PIC aiuta gli organi competenti a mettere in atto le diverse misure ed è responsabile segnatamente dei compiti seguenti:

- coordinamento delle misure per rafforzare la resilienza intersettoriale (tenuta dell'inventario PIC ecc.);
- sostegno alle autorità specializzate, di vigilanza e di regolazione competenti, nonché ai gestori nelle attività volte a verificare e rafforzare la resilienza delle infrastrutture critiche nei singoli settori;
- consulenza ai Cantoni nell'ambito di lavori rilevanti per la protezione delle infrastrutture critiche;
- preparazione dei dossier per le piattaforme di coordinamento;
- organo di contatto per le questioni PIC a livello nazionale e internazionale;
- redazione di rapporti sullo stato dell'attuazione della strategia nazionale PIC.

Le autorità responsabili di attuare le misure sono indicate nella strategia e nell'allegato 2. La resilienza specifica dei singoli settori (infrasettoriale) viene verificata e rafforzata in collaborazione con le autorità tecniche, di vigilanza e di regolamentazione corrispondenti, nonché con i gestori delle infrastrutture critiche (vedi allegato 1).

Si dovrà valutare se coinvolgere lo Stato maggiore federale Protezione della popolazione (SMF PP) (designazione attuale: Stato maggiore federale NBCN), in cui sono rappresentati i direttori di quasi tutti i settori rilevanti, come coordinatore dei lavori nel ruolo di comitato interdipartimentale (CI). Esso dovrebbe assumere in particolare il compito di sostenere, grazie a un controlling strategico, l'attuazione conforme agli obiettivi e alle tempistiche stabilite della strategia PIC.

Si tratta inoltre di valutare se affidare compiti PIC a una commissione extraparlamentare esistente. Questa dovrebbe garantire, a livello strategico, il coinvolgimento precoce dei gestori IC (spesso imprese private), dei cantoni nonché dell'economia e della società quali utenti delle IC. Essa deve inoltre assicurare che le necessarie conoscenze tecniche disponibili nei diversi settori confluiscano nella gestione strategica.

8.2 Tempistica e controlling

Le singole misure sono realizzate con l'ausilio di un piano d'attuazione e di controlling distinto, che sarà elaborato una volta approvata la strategia nazionale PIC. A grandi linee l'attuazione delle misure pianificabili dovrebbe avvenire con la seguente tempistica[3]:

Fase 1 (entro fine 2018)

- I piani d'attuazione sono elaborati.
- L'inventario PIC è rielaborato e completato con le imprese che gestiscono le IC. (M3)
- I processi per l'aiuto sussidiario ai gestori IC nella gestione degli eventi sono verificati e se necessario sono state formulate proposte di ottimizzazione. (M15)

Fase 2 (entro fine 2020)

- La valutazione di una base legale relativa all'obbligo di notifica in caso di interruzioni e perturbazioni è conclusa. (M2)
- È stata elaborata una proposta di base legale per il controllo di sicurezza su personale scelto dei gestori IC e altri titolari di autorizzazione d'accesso. (M10)
- Le basi per l'allacciamento dei gestori IC alla RDS sono state create. (M12).

Fase 3 (entro fine 2022)

- La resilienza dei sottosettori critici è stata verificata e sono state elaborate misure per rafforzarla. (M1)
- La valutazione di una base legale con disposizioni intersettoriali è conclusa. (M2)
- I risultati delle analisi a livello di sottosettori critici sono consolidati. (M4)

Il Consiglio federale è informato ogni due anni in merito allo stato d'attuazione delle misure.

3 I compiti permanenti come la gestione di piattaforme intersettoriali (M6) o l'integrazione di aspetti PIC nelle esercitazioni (M17) non figurano separatamente, ma sono integrati nel piano d'attuazione.

8.3 Revisione della strategia PIC

La strategia nazionale PIC tiene conto dei cambiamenti delle condizioni quadro e degli sviluppi contestuali e viene aggiornata se necessario. La presente strategia sarà verificata nel 2022 ed eventualmente adattata.

8 dicembre 2017

In nome del Consiglio federale svizzero:

La presidente della Confederazione, Doris Leuthard
Il cancelliere della Confederazione, Walter Thurnherr

Allegato 1

Descrizione dei sottosettori e competenze per il rafforzamento della resilienza nei settori critici (Misura 1)

Tabella 2

Descrizione dei sottosettori e delle relative competenze specifiche (Misura 1)

Settore	Sottosettore	Prestazioni particolarmente rilevanti dall'ottica PIC*	Organi federali competenti (elenco non esaustivo)**
Autorità	Ricerca e insegnamento	Prestazioni basate sulla ricerca in caso di catastrofi e situazioni d'emergenza (p. es. servizio sismico)	SEFRI
	Beni culturali	Garanzia della certezza del diritto (in part. archivi di Stato), identità	UFPP, UFC
	Parlamento, governo, giustizia, Amministrazione	Legislazione, guida e attuazione dei compiti dello Stato, giurisprudenza ed esecuzione delle leggi, compiti amministrativi generali (p. es. allerta e allarme in caso di pericolo, salvaguardia della sicurezza interna)	Servizi del Parlamento, CaF, DFAE, MeteoSvizzera, fedpol, SIO, SIC, AFF, ODIC e LE, UFAM
Energia	Approvvigionamento di gas	Commercio, trasporto, deposito e distribuzione di gas	UFE, IFO, UFAE
	Approvvigionamento di petrolio	Commercio, trasporto, deposito e distribuzione di combustibili e carburanti (benzina, cherosene, ecc.)	UFE, IFO, UFAE
	Approvvigionamento di elettricità	Produzione, commercio, trasporto, accumulazione e distribuzione di energia elettrica (senza alimentazione della linea ferroviaria)	UFE, ELCOM, ESTI, IFSN, UFAE
	Teleriscaldamento e calore di processo	Produzione e distribuzione di teleriscaldamento e calore di processo	UFE
Smaltimento	Rifiuti	Raccolta, eliminazione e riciclaggio di rifiuti speciali, delle economie domestiche e industriali	UFAM
	Acque di scarico	Smaltimento di acque luride delle economie domestiche, delle attività commerciali e delle industrie a protezione della popolazione (salute) e dell'ambiente	UFAM

Settore	Sottosettore	Prestazioni particolarmente rilevanti dall'ottica PIC*	Organi federali competenti (elenco non esaustivo)**
Finanze	Servizi finanziari	Svolgimento del traffico pagamenti, approvvigionamento della popolazione con denaro contante, capitalizzazione di terzi, raccolta di depositi e garanzia della stabilità dei prezzi	FINMA, AFF, SFI, UFAE, UFCOM
	Servizi assicurativi	Garanzia della protezione assicurativa, del sostegno finanziario in caso di sinistro e delle prestazioni nell'ambito della prevenzione dei sinistri (comprese assicurazioni malattia e assicurazioni sociali)	FINMA, AFF, SFI, UFAS
Sanità pubblica	Assistenza medica	Cure a domicilio, specialistiche e ospedaliere e cure veterinarie di base	SSC, UFSP
	Servizi di laboratorio	Analisi diagnostiche di laboratorio per la protezione dell'essere umano, degli animali e dell'ambiente	UFSP, USAV, UFPP
	Prodotti chimici e agenti terapeutici	Approvvigionamento con agenti terapeutici (farmaci e dispositivi medici), incl. vaccini	UFAE, Swissmedic, Farmacia dell'esercito
Informazione e comunicazione	Servizi informatici	Servizi informatici per l'economia (in part. elaborazione e archiviazione dati)	UFAE, ODIC
	Telecomunicazioni	Chiamate d'emergenza, Internet, diffusione di segnali radio e TV	UFCOM, UFAE
	Media	Informazione della popolazione in caso di catastrofi e situazioni d'emergenza, formazione dell'opinione politica	UFCOM
	Servizi postali	Servizi postali di base, in part. nel settore della corrispondenza ufficiale e commerciale	UFCOM, UFAE
Alimentazione	Approvvigionamento alimentare	Approvvigionamento della popolazione con derrate alimentari	UFAE, UFAG
	Approvvigionamento idrico	Approvvigionamento della popolazione e dell'economia con acqua potabile e di consumo	UFAM, UFAE

Settore	Sottosettore	Prestazioni particolarmente rilevanti dall'ottica PIC*	Organi federali competenti (elenco non esaustivo)**
Sicurezza pubblica	Esercito	Aiuto militare in caso di catastrofe, impieghi sussidiari di sicurezza, aiuto alla condotta per civili, difesa nazionale	Aggruppamento Difesa
	Organizzazioni di primo intervento (polizia, pompieri, sanità)	Garanzia della sicurezza pubblica, interventi di soccorso e di salvataggio, gestione di catastrofi e situazioni d'emergenza	fedpol, UFPP
	Protezione civile	Sostegno delle organizzazioni partner nella gestione di catastrofi e situazioni d'emergenza	UFPP
Trasporti	Traffico aereo	Trasporto di persone e merci via aria	UFAC, UFAE
	Traffico ferroviario	Trasporto di persone e merci su rotaia	UFT, UFAE
	Traffico navale	Trasporto di merci via acqua (in part. collegamento con i porti marittimi)	UFT, UFAE
	Traffico stradale	Trasporto di persone e merci su strada (trasporto motorizzato individuale e pubblico)	USTRA, UFAE

* Elenco non esaustivo; determinati obiettivi d'approvvigionamento sono definiti dall'organo competente (tra cui AEP).

** Gli organi citati determinano assieme al Segretariato PIC quali altri organi (Confederazione, Cantoni, associazioni ecc.) sono responsabili o devono essere coinvolti nel rafforzamento della resilienza. Le competenze vigenti sono mantenute.

Allegato 2

Panoramica delle misure, delle competenze e delle interfacce

Tabella 3

Misure, competenze e interfacce

Misura	Organi competenti (elenco non esaustivo)*	Interfacce con altri progetti / compiti / organi (non esaustivo)
M1: Verifica e rafforzamento della resilienza delle IC	Vedi allegato 1	SNPC, AEP, diversi progetti e compiti settoriali
M2: Esame base legale con direttive per gestori IC	UFPP, autorità specializzate, di vigilanza e di regolazione	SNPC
M3: Aggiornamento periodico Inventario PIC	UFPP	KATAPLAN, protezione contro i pericoli naturali
M4: Allestimento di un compendio dei rischi nei sottosettori critici	UFPP, ODIC, AFF	SNPC, gestione dei rischi Confederazione, AEP
M5: Approfondimento della ricerca fondamentale nel settore PIC	UFPP	Ricerca settoriale della Confederazione
M6: Gestione di piattaforme intersettoriali	UFPP	MELANI, AEP
M7: Verifica e aggiornamento periodico dei processi per l'informazione in caso d'evento	UFPP	MELANI
M8: Verifica dell'obbligo di notifica in caso di gravi incidenti e interruzioni	UFPP, ODIC	SNPC
M9: Verifica e aggiornamento periodico delle informazioni sul livello di sicurezza	UFPP, autorità specializzate, di vigilanza e di regolazione, UFAM	Protezione contro i pericoli naturali
M10: Elaborazione di una proposta di base legale per i controlli di sicurezza su personale scelto dei gestori IC e altri titolari di autorizzazione d'accesso	UFPP, SIO	LSIn
M11: Attuazione e aggiornamento periodico delle raccomandazioni relative alla priorizzazione delle IC in caso di penuria e interruzioni	UFAE, UFPP	AEP
M12: Realizzazione di una rete di dati a prova d'interruzione e creazione delle basi per l'allacciamento dei gestori IC	UFPP, Aggruppamento Difesa, Cantoni	RDS
M13: Elaborazione e aggiornamento dei piani preventivi per la gestione di interruzioni IC	Cantoni, enti specializzati, UFPP	KATAPLAN, piani preventivi della Confederazione, SMF PP
M14: Miglioramento della preparazione dello Stato, dell'economia e della popolazione	FPP, UFAE, CaF	Alertswiss, AEP

Misura	Organi competenti (elenco non esaustivo)*	Interfacce con altri progetti / compiti / organi (non esaustivo)
M15: Verifica e ottimizzazione dei processi per l'aiuto sussidiario dei gestori IC	UFPP, SG DDPS, fedpol	ResMaB, SMCP , SMF PP
M16: Elaborazione e aggiornamento dei piani d'intervento preventivi	Cantoni, ODIC, SG DDPS, UFPP	SNPC, KATAPLAN, PACD
M17: Integrazione di aspetti PIC nelle esercitazioni	UFPP, Cantoni, CaF, RSS	ECS, ERSS

* Il Segretariato PIC assume una funzione di coordinamento e assicura il coinvolgimento di tutti gli organi competenti e interessati.

Allegato 3

Elenco delle abbreviazioni

AEP	Approvvigionamento economico del Paese
AFF	Amministrazione federale delle finanze
BNS	Banca nazionale svizzera
CaF	Cancelleria federale
cfr.	confronta
D	Difesa
DATEC	Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DEFR	Dipartimento federale dell'economia, della formazione e della ricerca
DFF	Dipartimento federale delle finanze
DFGP	Dipartimento federale di giustizia e polizia
ecc.	eccetera
ECS	Esercitazione di condotta strategica
ElCom	Commissione federale dell'energia elettrica
ERSS	Esercitazione della Rete integrata Svizzera per la sicurezza
ESTI	Ispettorato federale degli impianti a corrente forte
fedpol	Ufficio federale di polizia
FINMA	Autorità federale di vigilanza sui mercati finanziari
FP	Fornitore di prestazioni
GPS	Global Positioning System
IC	Comitato interdipartimentale
IC	infrastruttura/e critica/che
IFO	Ispettorato federale degli oleo- e gasdotti
IFSN	Ispettorato federale della sicurezza nucleare
incl.	incluso
LAIn	Legge del 25 settembre 2015 sulle attività informative (RS *121*)
LPPC	Legge federale sulla protezione della popolazione e sulla protezione civile del 4 ottobre 2002 (RS *520.1*)
LSIn	Legge sulla sicurezza delle informazioni (disegno del Consiglio federale del 22 febbraio 2017, FF *2017* 2711)
MELANI	Centrale d'annuncio e d'analisi per la sicurezza dell'informazione
ODIC	Organo direzione informatica della Confederazione
p. es.	per esempio
PACD	Plan d'Action Cyber-Defence

PIC	Protezione delle infrastrutture critiche
ResMaB	Gestione federale delle risorse
risp.	rispettivamente
SEFRI	Segreteria di Stato per la formazione, la ricerca e l'innovazione
SFI	Segreteria di Stato per le questioni finanziarie internazionali
SG	Segreteria generale
SIC	Servizio delle attività informative della Confederazione
SIO	Sicurezza delle informazioni e degli oggetti
SMF NBCN	Stato maggiore federale pericoli nucleari, biologici, chimici e naturali (nuova denominazione: SMF PP)
SMF PP	Stato maggiore federale Protezione della popolazione
SNPC	Strategia nazionale per la protezione della Svizzera contro i cyberrischi
SSC	Servizio sanitario coordinato
TI	Tecnologia dell'informazione
TIC	Tecnologie dell'informazione e della comunicazione
UFAC	Ufficio federale dell'aviazione civile
UFAE	Ufficio federale per l'approvvigionamento economico del Paese
UFAG	Ufficio federale dell'agricoltura
UFAM	Ufficio federale dell'ambiente
UFC	Ufficio federale della cultura
UFCOM	Ufficio federale delle comunicazioni
UFE	Ufficio federale dell'energia
UFPP	Ufficio federale della protezione della popolazione
UFSP	Ufficio federale della sanità pubblica
UFT	Ufficio federale dei trasporti
USTRA	Ufficio federale delle strade